**EMERGENCY LETTER MOTION**

Feb 1, 2023

The Honorable Paul Adam Engelmayer
District Judge
Southern District of New York
40 Foley Square,
New York, New York

**Re: Emergency letter motion requesting Your Honor order ISPs to identify user(s) impersonating defendant to law enforcement agencies, mimicking violation of bond conditions**

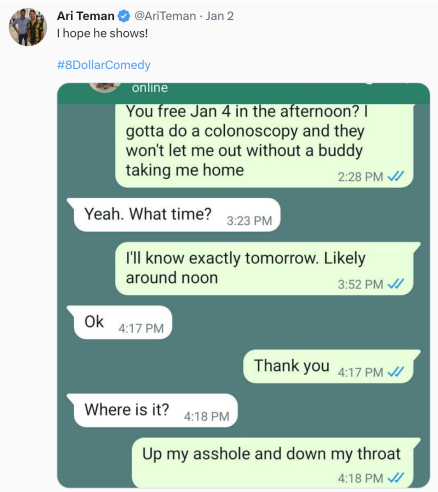
You Honor,

For the past number of months, and it appears likely for longer, an individual or individuals have been impersonating and using the Defendant's email address and social media to harass others and send messages to law enforcement agencies, the White House, law firms, and individuals, while pretending to be the defendant.

The perpetrators appear to monitor the defendant's social media and choose times the defendant will be offline, including when he is getting medical procedures under anesthesia, and on Jewish Holidays and Sabbaths when the defendant and many of his friends and family will not be online to alert him.

On January 4th, 2023, this individual(s) or entire sent messages using the defendant's email while the defendant was getting a routine colonoscopy for his 40th year checkup at University of Miami. When the defendant woke up, there were nearly a dozen messages from Federal law enforcement agencies (including but not limited-to: the DOJ and DEA) and even the White House, but also at-least one private law firm, confirming receipt of messages or sign-up requests.

The perpetrator would have known the Defendant would be offline because he'd tweeted that he was getting a colonoscopy that afternoon (please pardon the language of the joke):

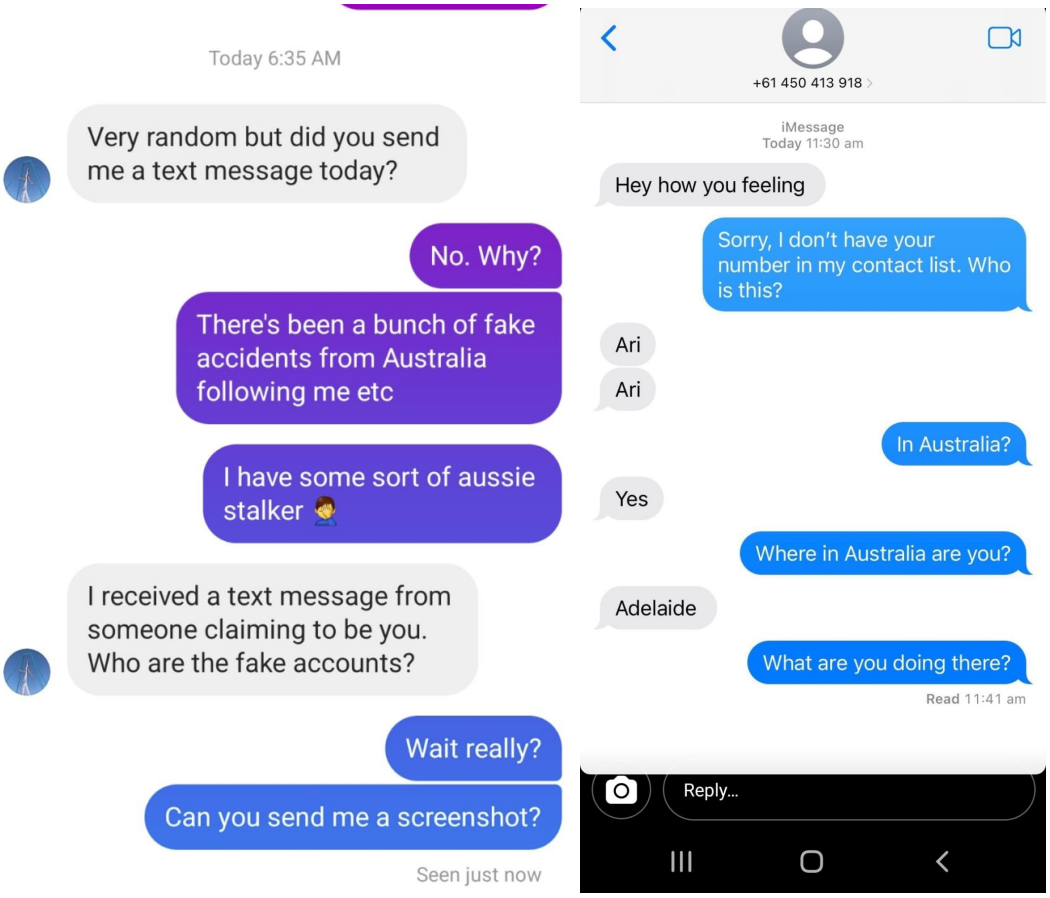



(source: https://twitter.com/AriTeman/status/1610085211051540485 )

Two service providers for these messaging platforms (Granicus and 123Greetings.com, Inc.) have provided the IP addresses of the individual(s), and they trace according to ARIN to T-Mobile users (e.g. https://search.arin.net/rdap/?query=172.58.228.71 ).

This fits a pattern over the past two years of similar messages and posts coinciding with times it would be publicly known the defendant was offline. This also includes a young woman in Australia, whom I'd dated a while ago, who reported text messages from someone claiming to be Ari, who appears to have used "spoofed" numbers.

For example:




Private detectives confirmed that the number was spoofed (the actual owner of the number is a business and was not involved at all) and could have come from anywhere in the world, including the United States. The only way this individual would know to contact this young lady pretending to be the Defendant is if they had unauthorized access to my accounts or social media.

Needless to say, someone harassing past relationships puts the Defendant at risk of being accused of violating bond conditions.

There are other incidents, but these should suffice, we hope, to persuade Your Honor that attempting to identify this imposter and harasser is important to protect the Defendant and those whom this imposter is messaging.

**Because the defendant's bond conditions require notifying Pretrial Services of any law enforcement interactions,** this topic is well within Your Honor's jurisdiction due to the messages to the DOJ, DEA, and

White House, and we ask Your Honor to order T-Mobile, Google, Apple, and Meta to provide the name(s), number(s), username(s), addresses on record, and any and all GPS coordinates of the users of IP 172.56.34.78 and 172.58.228.71 from January 4th and 5th, 2023, and any other relevant information. The Defendant will then seek a restraining order based on this information, if appropriate.

We are in contact with T-Mobile, for example, but these organizations request Subpoenas or Court Orders to provide this information.

We thank Your Honor for your prompt attention to this matter so we can prevent escalation and further harassment by this stalker.

**Officer Bostic of Pretrial Services have confirmed that they do not oppose this motion, they take no position.**

Oddly, and the Defendant concedes that this entire scenario is also very strange, Mr. Bhatia is refusing to consent to this motion, which is all the more strange because the IP address of the imposter traces to “City Hall Park” which is near his offices -- perhaps he knows who the imposter is and does not want us to know or wishes to delay us finding out, since we will anyway. I would therefore ask that you require AUSA Mr. Bhatia, AUSA Mr. Gutwillig, and AUSA Ms. Graham in their reply to this emergency motion to issue a statement under penalty of perjury as to whether they know who the imposter is and whether or not it is them or an associate of theirs.

**Two draft orders are below for Your Honor’s convenience.**

Thank you,

s/Ari Teman/

Defendant, Pro Se

_____

**DRAFT ORDER TO SDNY**

The Court orders Mr. Bhatia, Mr. Gutwillig, Ms. Graham and any staff member of the United States Attorneys Office for the Southern District of New York involved in *United States v Teman* in the District Court or the Second Circuit Appeal to attach a sworn statement under penalty of perjury to a reply to this motion confirming that they do not know the identity(s) of the imposter(s) referenced by this motion, and that they are not in any way involved in impersonating Mr. Teman in any way.

They should also provide a clear and detailed statement as to why they oppose an order exposing the identity of the imposter(s) who has allegedly impersonated Mr. Teman to Federal Agencies, the White House, and others.

The Court orders the Government to reply to this motion by February 3rd, 2023 at 4pm.

So Ordered

The Honorable Paul Engelmayer

_____

February ____ 2023

**DRAFT ORDER TO THE ISPS**

The Court orders T-Mobile, Meta, Google, Apple Inc, and any and all of their subsidies, Partners, and vendors to provide the following information to Ari Teman (ari@teman.com) and Attorney Eden Quainton (equainton@gmail.com) by Feb 8, 2023, for the IP addresses 172.56.34.78 and 172.58.228.71 (and any others which are determined relevant in the course of your investigations) especially during January 4th and 5th, 2023, but also any dates from May 10, 2019 until today:

> Names, email addresses, GPS coordinates and any other location data, device information, full activity logs, usernames, any purchasing information (location, method, any details on the purchasing of the devices used), call and message logs (all formats),
>
> and any other information which may be helpful to identify the individual or individuals or entities impersonating or stalking Mr. Teman, such as but not limited to using his email addresses, accessing his and/or his companies' social media accounts, accessing or tampering with his phone or devices.

Should it be determined that these IP addresses were "spoofed", these companies should make an effort to provide the actual IP addresses used and the relevant information as such, which they can do by following the traffic to these services (Granicus and _) during the relevant times.

So ordered,

The Honorable Paul Engelmayer

_____

February ____ 2023